



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/566,728

02/02/2006

Tomoaki Ryu

11900618PUS1

9704

2292 7590 01/13/2010
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER

POGMORE, TRAVIS D

ART UNIT

PAPER NUMBER

2436

NOTIFICATION DATE

DELIVERY MODE

01/13/2010

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No. 10/566,728	Applicant(s) RYU, TOMOAKI	
	Examiner Travis Pogmore	Art Unit 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 August 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 7, 8, 10 and 11 is/are rejected.
- 7) ☒ Claim(s) 6 and 9 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-11 are currently pending.
2. Applicant's arguments, with regards to claims 1-11, filed August 5, 2009 have been fully considered but they are not wholly persuasive.

Examiner Notes

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Objections

4. Claims 6 and 9 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections – 35 USC § 103

5. Claims 1-5, 7-8 and 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 4,907,275 (hereinafter "Hashimoto") in view of U.S. Patent No. 5,392,351 (hereinafter "Hasebe") in further view of U.S. Patent No. 7,230,898 (hereinafter "Yokota").

As to claim 1, Hashimoto teaches a digital recording apparatus comprising:

Art Unit: 2436

a data control circuit which receives a digital recording signal (Fig. 1, elements 17 and 19);

a memory which is capable of communicating information with the data control circuit (Fig. 1, elements 14 and 16);

an encryption circuit which is capable of communicating information with the data control circuit, the encryption circuit encrypting the digital recording signal (Fig. 1, element 4); and

a recording signal processing circuit which causes the data control circuit to control transmission of the digital recording signal (Fig. 2a, element 10, the CPU of the computer system), but does not specifically teach the recording unit which is controlled by the data control circuit, the recording unit recording the digital recording signal on a recording medium, the encryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted, or wherein when the digital recording signal needs to be encrypted, the encryption circuit begins to start up and the digital recording signal is transmitted from the data control circuit to the memory to be stored in the memory during start-up of the encryption circuit, and when the encryption circuit becomes capable of operation, the digital recording signal stored in the memory is transmitted via the data control circuit to the encryption circuit and is encrypted by the encryption circuit to be recorded in a recording unit.

However, Hasebe teaches a recording unit which is controlled by the data control circuit, the recording unit recording the digital recording signal on a recording medium is well known and expected in the art (Fig. 4, element S6, column 9, line 66 to column 10,

Art Unit: 2436

line 15, in order to record encrypted information on the storage medium it must inherently have a recording unit).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to record the signal on a recording medium as in Hasebe because this is a well known and expected addition to general purpose computers.

Furthermore, Yokota teaches the encryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38); and

wherein when the digital recording signal needs to be encrypted, the encryption circuit begins to start up and the digital recording signal is transmitted from the data control circuit to the memory to be stored in the memory during start-up of the encryption circuit, and when the encryption circuit becomes capable of operation, the digital recording signal stored in the memory is transmitted via the data control circuit to the encryption circuit and is encrypted by the encryption circuit to be recorded in a recording unit (Fig. 3, Fig. 11, elements S104 to S106, and column 15, line 50 to column 16, line 17, the data (i.e., digital recording signal) being retrieved from stick-shaped memory 1 (i.e., the memory), and passed through CPU 41 (i.e., the data control circuit) to enter the encryption/decryption circuit 60).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this “translates into a reduction of power

Art Unit: 2436

consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery” (Yokota, column 16, lines 39-42).

As to claim 2, Hashimoto teaches a digital reproducing apparatus comprising:
a data control circuit which controls the reproducing unit and outputs a reproduced digital recording signal (Fig. 2a, element 10, the CPU controlling every part of the computer system);

a memory which is capable of communicating information with the data control circuit (Fig. 1, elements 14 and 16);

a decryption circuit which is capable of communicating information with the data control circuit, the decryption circuit decrypting the digital recording signal (Fig. 1, element 4 and column 1, lines 52-58, as substantially similar hardware and process is used for decryption the encryption circuit also acts as a decryption circuit); and

a recording signal processing circuit which causes the data control circuit to control transmission of the digital recording signal (Fig. 2a, element 10, the CPU), but does not teach a reproducing unit which reproduces a digital recording signal from a recording medium, the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted, or wherein when the digital recording signal encrypted and recorded on the recording medium needs to be decrypted and reproduced, during start-up of the decryption circuit, the digital recording signal having been stored before start-up of the decryption circuit is outputted via the data control circuit, and when the decryption circuit is capable of operation, the digital

Art Unit: 2436

recording signal read by the reproducing unit is transmitted via the data control circuit to the decryption circuit and is decrypted by the decryption circuit to be outputted.

However Hasebe teaches a reproducing unit which reproduces a digital recording signal from a recording medium (column 9, line 66 to column 10, line 15, the reproducing unit comprising the "optical magnetic apparatus" for the appropriate medium of an "optical magnetic disk").

. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to reproduce a signal from a recording medium as in Hasebe because his is a well known and expected addition to general purpose computers.

Furthermore, Yokota teaches the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38); and

wherein when the digital recording signal encrypted and recorded on the recording medium needs to be decrypted and reproduced, during start-up of the decryption circuit, the digital recording signal having been stored before start-up of the decryption circuit is outputted via the data control circuit, and when the decryption circuit is capable of operation, the digital recording signal read by the reproducing unit is transmitted via the data control circuit to the decryption circuit and is decrypted by the decryption circuit to be outputted (Fig. 3, Fig. 11, elements S104 to S106, and column 15, line 50 to column 16, line 17, the data (i.e., digital recording signal) being retrieved

Art Unit: 2436

from stick-shaped memory 1 (i.e., the memory), and passed through CPU 41 (i.e., the data control circuit) to enter the encryption/decryption circuit 60).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this “translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery” (Yokota, column 16, lines 39-42).

As to claim 3, Hashimoto teaches a digital recording/reproducing apparatus comprising:

the digital recording apparatus of claim 1 (as taught by Hashimoto, Hasebe and Yokota above); and

a digital reproducing apparatus comprising:

a data control circuit which controls the reproducing unit and outputs a reproduced digital recording signal (Fig. 2a, element 10, the CPU controlling every part of the computer system);

a memory which is capable of communicating information with the data control circuit (Fig. 1, elements 14 and 16);

a decryption circuit which is capable of communicating information with the data control circuit, the decryption circuit decrypting the digital recording signal (Fig. 1, element 4 and column 1, lines 52-58, as substantially similar hardware and process is used for decryption the encryption circuit also acts as a decryption circuit); and

a recording signal processing circuit which causes the data control circuit to control transmission of the digital recording signal (Fig. 2a, element 10, the CPU), but does not teach a reproducing unit which reproduces a digital recording signal from a recording medium, the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted, or wherein when the digital recording signal encrypted and recorded on the recording medium needs to be decrypted and reproduced, during start-up of the decryption circuit, the digital recording signal having been stored before start-up of the decryption circuit is outputted via the data control circuit, and when the decryption circuit is capable of operation, the digital recording signal read by the reproducing unit is transmitted via the data control circuit to the decryption circuit and is decrypted by the decryption circuit to be outputted.

However Hasebe teaches a reproducing unit which reproduces a digital recording signal from a recording medium (column 9, line 66 to column 10, line 15, the reproducing unit comprising the "optical magnetic apparatus" for the appropriate medium of an "optical magnetic disk").

. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to reproduce a signal from a recording medium as in Hasebe because his is a well known and expected addition to general purpose computers.

Furthermore, Yokota teaches the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38); and

wherein when the digital recording signal encrypted and recorded on the recording medium needs to be decrypted and reproduced, during start-up of the decryption circuit, the digital recording signal having been stored before start-up of the decryption circuit is outputted via the data control circuit, and when the decryption circuit is capable of operation, the digital recording signal read by the reproducing unit is transmitted via the data control circuit to the decryption circuit and is decrypted by the decryption circuit to be outputted (Fig. 3, Fig. 11, elements S104 to S106, and column 15, line 50 to column 16, line 17, the data (i.e., digital recording signal) being retrieved from stick-shaped memory 1 (i.e., the memory), and passed through CPU 41 (i.e., the data control circuit) to enter the encryption/decryption circuit 60).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this “translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery” (Yokota, column 16, lines 39-42).

As to claim 4, Hashimoto teaches an encryption apparatus comprising:
a storage unit which stores a digital signal (Fig. 1, elements 14 and 16);
an encryption unit which encrypts the digital signal (Fig. 1, element 4);
a determination unit which determines whether or not the digital signal needs to be encrypted by the encryption unit (Fig. 1, elements 3 and 18, and column 6, lines 25-60, the logic circuit and the selector being the determination unit), but does not

Art Unit: 2436

specifically teach an encryption key generation unit which generates an encryption key for enabling the encryption unit, the encryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted, or a control unit which controls the storage unit and the encryption unit in such a way that when the determination unit determines that the digital signal does not need to be encrypted, the digital signal is not encrypted by the encryption unit and the digital signal stored in the storage unit is outputted, and when the determination unit determines that the digital signal needs to be encrypted, the digital signal from a time of the determination to a time when the enabling of the encryption unit is completed by the encryption key is stored in the storage unit and is encrypted by the encryption circuit to be outputted after the enabling of the encryption unit is completed.

However Hasebe teaches an encryption key generation unit which generates an encryption key for enabling the encryption unit (column 4, lines 31-48, encryption being the role of the "vendor computer").

. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to include a key generation unit as in Hasebe because this increases security by keeping all steps of the encryption process inside a single computer.

Furthermore, Yokota teaches the encryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38); and

Art Unit: 2436

a control unit which controls the storage unit and the encryption unit in such a way that when the determination unit determines that the digital signal does not need to be encrypted, the digital signal is not encrypted by the encryption unit and the digital signal stored in the storage unit is outputted, and when the determination unit determines that the digital signal needs to be encrypted, the digital signal from a time of the determination to a time when the enabling of the encryption unit is completed by the encryption key is stored in the storage unit and is encrypted by the encryption circuit to be outputted after the enabling of the encryption unit is completed (Fig. 3, Fig. 11, elements S104 to S106, and column 15, line 50 to column 16, line 17, the data (i.e., digital recording signal) being retrieved from stick-shaped memory 1 (i.e., the memory), and passed through CPU 41 (i.e., the data control circuit) to enter the encryption/decryption circuit 60).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this “translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery” (Yokota, column 16, lines 39-42).

As to claim 5, Hasebe teaches wherein the encryption key is generated from information read from a recording medium for recording the digital signal (column 4, lines 31-48).

Art Unit: 2436

As to claim 6, wherein when the determination unit determines that the digital signal needs to be encrypted, the storage unit secures a vacant capacity larger than a capacity capable of storing the digital signal from a time of the determination to a time when the enabling of the encryption unit is completed by the encryption key is well known and expected in the art (e.g. U.S. Patent No. 5,303,302, column 3, lines 40-59, in particular the third recited embodiment discloses a standard method of ensuring enough space to avoid a buffer overflow, and as in the invention described in Hashimoto, column 3, lines 1-15, the buffer must be able to store sufficient data for it to be correctly processed).

As to claim 7, Hashimoto teaches a decryption apparatus comprising:

a storage unit which stores a digital signal (Fig. 1, elements 14 and 16);

a decryption unit which decrypts an encrypted signal of the digital signal (Fig. 1, element 4 and column 1, lines 52-58, as substantially similar hardware and process is used for decryption the encryption circuit also acts as a decryption circuit);

a determination unit which determines whether or not the digital signal needs to be decrypted by the decryption unit (Fig. 1, elements 3 and 18, and column 6, lines 25-60, the logic circuit and the selector being the determination unit), but does not specifically teach an encryption key generation unit which generates an encryption key for enabling the decryption, the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted, or a control unit which controls the storage unit and the decryption unit in such a way that when the

Art Unit: 2436

determination unit determines that the digital signal does not need to be decrypted, the digital signal is not decrypted by the decryption unit and the digital signal stored in the storage unit is outputted, and when the determination unit determines that the digital signal needs to be decrypted, the digital signal from a time of the determination to a time when the enabling of the decryption unit is completed by the encryption key is stored in the storage unit and is decrypted by the decryption circuit to be outputted after the enabling of the decryption unit is completed.

However Hasebe teaches an encryption key generation unit which generates an encryption key for enabling the decryption (column 4, lines 31-48, decryption being the role of the "user computer").

. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to include a key generation unit as in Hasebe because this increases security by keeping all steps of the encryption process inside a single computer.

Furthermore, Yokota teaches the decryption circuit being deactivated before the data control circuit receives the digital recording signal to be encrypted (column 16, lines 32-38); and

a control unit which controls the storage unit and the decryption unit in such a way that when the determination unit determines that the digital signal does not need to be decrypted, the digital signal is not decrypted by the decryption unit and the digital signal stored in the storage unit is outputted, and when the determination unit determines that the digital signal needs to be decrypted, the digital signal from a time of

Art Unit: 2436

the determination to a time when the enabling of the decryption unit is completed by the encryption key is stored in the storage unit and is decrypted by the decryption circuit to be outputted after the enabling of the decryption unit is completed (Fig. 3, Fig. 11, elements S104 to S106, and column 15, line 50 to column 16, line 17, the data (i.e., digital recording signal) being retrieved from stick-shaped memory 1 (i.e., the memory), and passed through CPU 41 (i.e., the data control circuit) to enter the encryption/decryption circuit 60).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this “translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery” (Yokota, column 16, lines 39-42).

As to claim 8, Hasebe teaches wherein the encryption key is generated from information read from a recording medium for recording the digital signal (column 4, lines 31-48).

As to claim 9, wherein when the determination unit determines that the digital signal needs to be decrypted, the amount of data of the digital signal stored in the storage unit is not less than an amount of data outputted from a time of the determination to a time when the enabling of the decryption unit is completed by the encryption key is well known and expected in the art (e.g. U.S. Patent No. 5,303,302,

Art Unit: 2436

column 3, lines 40-59, in particular the third recited embodiment discloses a standard method of ensuring enough space to avoid a buffer overflow, and as in the invention described in Hashimoto, column 3, lines 1-15, the buffer must be able to store sufficient data for it to be correctly processed).

As to claim 10, Hashimoto teaches an encryption method comprising the steps of:

storing a digital signal (Fig. 1, elements 14 and 16);

encrypting the digital signal (Fig. 1, element 4); and

determining whether or not the digital signal needs to be encrypted (Fig. 1, elements 3 and 18, and column 6, lines 25-60, the logic circuit and the selector being the determination unit), but does not specifically teach generating an encryption key for enabling a function of encrypting the digital signal, or wherein when the determination is that the digital signal does not need to be encrypted, the digital signal is not encrypted and the stored digital signal is outputted, and when the determination is that the digital signal needs to be encrypted, the digital signal from a time of the determination to a time when the function of encrypting is enabled is stored and is encrypted to be outputted after the enabling of the function of encrypting is completed.

However, Hasebe teaches generating an encryption key for enabling a function of encrypting the digital signal (e.g. column 4, lines 31-48, encryption being the role of the "vendor computer").

Art Unit: 2436

. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to generate a key as in Hasebe because this increases security by keeping all steps of the encryption process inside a single computer.

Furthermore, Yokota teaches wherein when the determination is that the digital signal does not need to be encrypted, the digital signal is not encrypted and the stored digital signal is outputted, and when the determination is that the digital signal needs to be encrypted, the digital signal from a time of the determination to a time when the function of encrypting is enabled is stored and is encrypted to be outputted after the enabling of the function of encrypting is completed (Fig. 3, Fig. 11, elements S104 to S106, and column 15, line 50 to column 16, line 17, the data (i.e., digital recording signal) being retrieved from stick-shaped memory 1 (i.e., the memory), and passed through CPU 41 (i.e., the data control circuit) to enter the encryption/decryption circuit 60).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this “translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery” (Yokota, column 16, lines 39-42).

As to claim 11, Hashimoto teaches a decryption method comprising the steps of: storing a digital signal (Fig. 1, elements 14 and 16);

Art Unit: 2436

decrypting an encrypted digital signal of the digital signal (Fig. 1, element 4 and column 1, lines 52-58, as substantially similar hardware and process is used for decryption the encryption circuit also acts as a decryption circuit); and

determining whether or not the digital signal needs to be decrypted (Fig. 1, elements 3 and 18, and column 6, lines 25-60, the logic circuit and the selector being the determination unit), but does not specifically teach generating an encryption key for enabling a function of decrypting the digital signal, or wherein when the determination is that the digital signal does not need to be decrypted, the digital signal is not decrypted and the stored digital signal is outputted, and when the determination is that the digital signal needs to be decrypted, the digital signal from a time of the determination to a time when the function of decrypting is enabled is stored and is decrypted to be outputted after the enabling of the function of decrypting is completed.

However, Hasebe teaches generating an encryption key for enabling a function of decrypting the digital signal (column 4, lines 31-48, decryption being the role of the "user computer").

. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to generate a key as in Hasebe because this increases security by keeping all steps of the encryption process inside a single computer.

Furthermore, Yokota teaches wherein when the determination is that the digital signal does not need to be decrypted, the digital signal is not decrypted and the stored digital signal is outputted, and when the determination is that the digital signal needs to

Art Unit: 2436

be decrypted, the digital signal from a time of the determination to a time when the function of decrypting is enabled is stored and is decrypted to be outputted after the enabling of the function of decrypting is completed (Fig. 3, Fig. 11, elements S104 to S106, and column 15, line 50 to column 16, line 17, the data (i.e., digital recording signal) being retrieved from stick-shaped memory 1 (i.e., the memory), and passed through CPU 41 (i.e., the data control circuit) to enter the encryption/decryption circuit 60).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Hashimoto to activate the encryption circuit only as needed as in Yokota because this “translates into a reduction of power consumption ... [and] when this embodiment operates from a battery unit, the process helps prolong the life of the battery” (Yokota, column 16, lines 39-42).

Response to Arguments

6. On pages 2-4 of the Pre-Brief Conference Request, Applicant argues that Hashimoto does not teach processing a digital recording/reproduction signal during the time period when an encryption/decryption circuit is starting up.

7. Applicant’s arguments, have been fully considered and are persuasive.

Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of a newly cited portion of Yokota regarding the claim limitations at issue.

8. Therefore, in view of the above reasons, Examiner maintains rejections as noted above.

Art Unit: 2436

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Travis Pogmore whose telephone number is 571-270-7313. The examiner can normally be reached on Monday through Thursday between 9:30 a.m. and 4:00 p.m. eastern time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/Travis Pogmore/
Examiner, Art Unit 2436

Application/Control Number: 10/566,728
Art Unit: 2436

Page 20